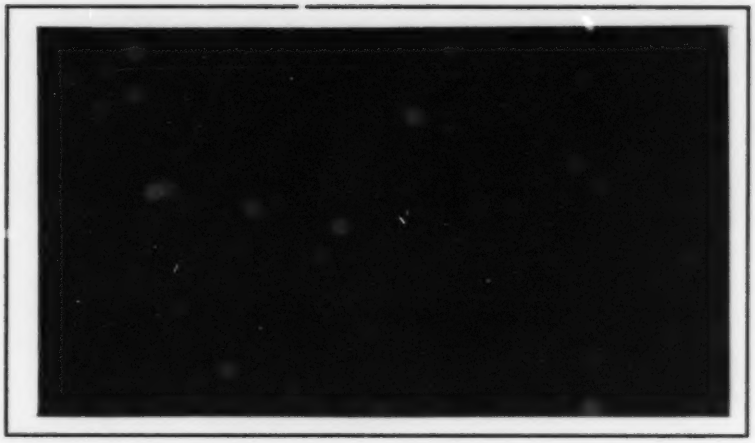

CENTRE FOR
SYSTEMS
SCIENCE

LCCR

Simon Fraser University, Burnaby, B.C., Canada V5A 1S6 / (604) 291-4704

Notes on Multiple Input Signature Analysis

Tiko Kameda/Slawomir Pilarski/Andre Ivanov

CSS/LCCR TR90-16

July 1990

92-05800/

Notes on Multiple Input Signature Analysis*

Tiko Kameda†, Slawomir Pilarski‡ and Andre Ivanov‡

Abstract

In built-in self-test (BIST), a large number of test patterns are applied to the circuit under test, and the response data are compacted by a finite state machine into a signature of a small number of bits. Determining the amount of aliasing introduced by compaction is crucial for establishing the test quality. Many results regarding the probability of aliasing for multiple-input compactors have been derived from error assumptions that are not very realistic for VLSI circuits. Very recently, however, two research groups have independently proved the following: the value of aliasing probability tends to 2^{-k}, where k is the number of binary memory elements of the linear compactor, provided that the compactor is characterized by an irreducible polynomial and that the "no error" vector has a probability different from zero. In these notes we generalize the above result and prove that it is valid if any two error vectors, neither of which need to be the "no error" vector, have probabilities of occurrence different from zero. To make the error model complete, we also consider the situation in which exactly one error vector has a probability different from zero. For such error distributions, we determine the times at which aliasing occurs. Simple proofs for the results are provided, based on standard linear algebra notions and well-known theorems.

1 Introduction

The last decade has seen a multitude of chip and board-level design-for-testability techniques proposed, implemented, and, in some cases, adopted as standards [10, 16, 31].

*This work was partially supported by grants from the Natural Sciences and Engineering Research Council of Canada and the Advanced Systems Institute of British Columbia.

†School of Computing Science, Simon Fraser University, Burnaby, B.C., Canada V5A 1S6

‡Department of Electrical Engineering, University of British Columbia, B.C., Canada V6T 1W5

Among these, built-in self-test (BIST) [1] is emerging as one of the most promising solutions for testing large and complex integrated circuits [32]. In BIST, during a testing session, a circuit under test (CUT) is stimulated by a set of test patterns, generated by a built-in test pattern generator. For practical reasons, the generally large amount of test response data produced by a CUT is usually compacted by a built-in test response compactor. Several compaction techniques have been proposed for BIST. The one that has received the most attention is known as *signature analysis* [9], though several other techniques and their combinations have been proposed [1, 3, 12, 14, 19, 20, 23, 30].

In spite of their specific differences, each of the compaction techniques proposed to date uses some form of a finite state machine (FSM) that is initialized and then undergoes a sequence of state transitions as the sequence of test response vectors produced by the CUT is applied to its inputs. We call such an FSM a *compacting finite state machine* (CFSM). At the end of a testing session, the final state of a CFSM is checked, thereby constituting the basis for the pass/fail analysis. Since the number of storage elements, e.g., flip-flops, of a CFSM is generally small compared with the number of bits in the test response sequence, compaction may imply an information loss, such that a faulty circuit that produces an erroneous test response may yield the same final state as its fault-free counterpart. Such a situation leads to an incorrect pass/fail decision, and is referred to as an *aliasing* error.

Given a specific circuit to which a specific test sequence is applied and for which the responses are compacted by a specific CFSM, it is possible to determine which faults among a given set will not be detectable due to aliasing. Thus, it is possible to determine the *aliasing ratio*, i.e., the fraction of faults that cause erroneous test response sequences but are not detectable because of aliasing. The greater the aliasing ratio, then the greater will be the number of faulty chips that can potentially pass the testing procedure. Hence, the aliasing ratio, like test pattern generation effectiveness, affects test quality. Unfortunately, detailed circuit simulation required for obtaining a precise value of the aliasing ratio is very expensive, especially for large circuits. The aliasing ratio is therefore generally estimated by a probability, referred to as the *aliasing probability*, e.g., [7, 29].

The determination of the aliasing probability associated with the different com-

paction schemes for BIST has attracted much recent research interest. Earlier findings were based on not very realistic assumptions, or were only applicable to limited cases such as single-output CUTs. More recent efforts have made attempts at generalizing these earlier results. This paper presents such a generalization regarding the aliasing probability associated with signature analysis for multiple-output CUTs. The result applies, for example, to multiple-input signature registers [1] and cellular automata [14].

The remainder of this paper is organized as follows. Sec. 2 presents a summary of some related work, and further motivates the subsequent sections. Sec. 3 contains preliminaries, namely, some definitions and linear algebraic notions that are used in the subsequent section to prove the principal results of the paper. Sec. 4 presents those principal results by stating properties of linear compactors that are characterized by irreducible polynomials. The probabilistic implications of our theorems are also included in this section. Sec. 5 provides further discussion of the results, and comments on other approaches recently taken to prove less general results than those that we present here. Finally, Sec. 6 concludes the paper.

2 Related Work and Motivation

A number of papers have been published on the probability of aliasing for different compaction techniques. The majority of them treat aliasing associated with signature analysis. Moreover, thus far, the majority of papers on signature analysis considered the probability of aliasing for single-input signature analyzers, which most naturally apply to single-output CUTs. However, practically all VLSI circuits are multiple-output. There exist several different ways of compacting the output responses of multiple-output CUTs. One simple way is to use a multiple-input linear feedback shift register (MISR), where the outputs of the CUT feed the inputs of the MISR directly (see [1]).

In general, to determine the aliasing probability, an error model that describes the behavior of a faulty circuit is needed. The error model characterizes possible error sequences and the distribution of their probabilities. Earlier work, e.g., [11, 24], on the aliasing probability of MISRs assumed equally-likely errors. Under this assumption, the aliasing probability can be shown to tend to 2^{-k}. However, this error assumption is

not considered as a realistic model of faulty CUTs. More recently, several papers have assumed that errors appear at different outputs of the CUT independently with possibly different probabilities. Under this assumption, it has been shown that for any MISR, if all possible error patterns have probabilities different from zero and one, then the aliasing probability tends to 2^{-k} as the test sequence length tends to infinity [28]. This asymptotic value was also shown to hold even if, at some outputs, the probability of an error is zero or one, provided that the MISR is characterized by a primitive characteristic polynomial [5].

The weakness in the above error models lies in the assumption of independence of the errors occurring at different outputs. Most CUTs will have potential faults that lead to correlated errors at their outputs. In [15, 18, 22], an error model that allows for correlated errors at the outputs is considered. This model is the well-known *symmetric q-ary* communication channel error model [21], where $q = 2^k$, and k corresponds to the number of CUT outputs in the case of circuit testing. In this error model, it is assumed that the error-free response has probability p_0, and each of the remaining $2^k - 1$ error patterns has probability $(1 - p_0)/2^k - 1$. Under this assumption, it has also been shown that the aliasing probability tends to 2^{-k}, as the test sequence length tends to infinity.

Though the q-ary symmetric channel error model allows for possible correlations of errors at the different outputs of a CUT, its weakness lies in that it assumes all error patterns to have a non-zero probability of occurrence, and moreover, assumes each to be equally-likely. These two assumptions are not necessarily realistic. Aliasing associated with MISRs, as well as with other linear compactors such as cellular automata [14], assuming possible correlations, was studied in [27]. In the latter, it was shown that the aliasing probability tends to 2^{-k} as the test length tends to infinity, irrespectively of the error distribution, provided that the markov process underlying the compaction process is ergodic and doubly stochastic [8].

For some linear compaction machines and some error distributions, it is possible for the underlying Markov process not to be ergodic. In that case, the aliasing probability may tend to a value greater than 2^{-k}. This has been observed in [13] and [5]. For some error distributions, it is also possible that for a given test length, the aliasing probability

is either zero or one.

In practice, for the purpose of establishing the test quality of a BIST strategy, one is not interested in the performance of the strategy with respect to an error model, but rather in its performance with respect to a predefined fault set. In most papers, however, it is not explicitly stated how the derived results extend or apply to fault sets. To generalize the results to the fault sets, different possibilities exist.

One possibility is to average the distribution of errors for all the faults of the circuit, and then determine the corresponding probability of aliasing. Since finding the exact error distribution for all the faults is computationally intractable, an average distribution may be assumed or estimated. The total number of faults that would cause aliasing is then determined from this average aliasing probability. This approach has been considered in [18]. However, this approach can possibly lead to optimistic conclusions. That is, if the average of the error distribution is taken, then a nonzero probability of error will result at each of the circuit outputs. In that case, it has been shown that the aliasing probability tends to 2^{-k} regardless of the characteristic polynomial of the MISR. However, it has also been shown that it is possible, in the case of MISRs not characterized by irreducible polynomials, for some faults to have a probability of aliasing that exceeds 2^{-k}. Thus, if a circuit had many faults resulting in such error distributions, which is probable, then the overall aliasing ratio could be much greater than expected.

A better second alternative is to determine the error distribution for each fault in a circuit, and to determine the corresponding probability of aliasing. The overall probability of aliasing can then be taken as the average of the aliasing probability for each of the faults. The major problem with this approach, however, is its computational intractability. That is, finding the error distribution for each of the faults in a large circuit is generally not practical. In fact, it would require exact fault simulation for each of the faults, which is precisely what the probabilistic solutions to the aliasing problem are intended to avoid.

Thus, a third alternative is to guarantee that, for *each* of the possible faults in a circuit, i.e., regardless of the error distribution, the aliasing probability is either zero or asymptotically 2^{-k}. In the remainder of this paper, we prove that this is possible

for a certain class of CFSMs, namely, those represented by matrices with irreducible characteristic polynomials. Similar results have recently been obtained by others [4, 6]. However, the error model considered in [4, 6] does not include all possible error distributions. For example, consider a circuit with an output that produces a 1 for only a few input vectors. If all the input test patterns applied to the CUT produce a 0 at this particular output, if the CUT were fault-free, then in the case of a stuck-at-1 fault on this output, every output vector produced by the CUT would be erroneous. Thus, the error vector distribution for this fault would consist of a single error vector, with a probability of occurrence equal to one. It is also possible for certain faults (single or multiple) to yield a distribution of error vectors where the "no-error" vector is not part of the distribution. Here, we consider such possible distributions that neither [4] nor [6] considers. We show that the 2^{-k} asymptotic result holds for any distribution of two or more vectors. For distributions of only one vector, the aliasing probability is either one or zero, depending on the error vector, the test length, and the state cycle structure of the compactor. We give criteria that enable one to avoid the test lengths for which aliasing is possible.

The practical significance of the result is considerable, since it identifies which CFSM implementations ensure that the aliasing probability asymptotically reaches 2^{-k} for faults that can produce more than one error vector, and states for which test lengths aliasing is impossible for faults that produce exactly one error vector. As discussed above, such information may be the only information on aliasing available to a circuit designer, especially at an early design stage.

3 Preliminaries

Among the various CFSMs proposed in the past for BIST, the best known are multiple input signature registers (MISRs) with their several different possible implementations, e.g., [1, 26]. Another type of CFSM used for BIST is based on cellular automata [14]. These CFSMs are representatives of a more general class of compactors, i.e., linear compactors, defined below.

We consider the states of a CFSM as elements of a k-dimensional vector space

$\Theta_k = \{0,1\}^k$ over the Galois field, GF(2), with binary addition "+" and multiplication "$\cdot$".[1] Θ_k thus consists of 2^k vectors. Both the state s of a CFSM and the response r from the CUT belong to Θ_k. In the following, unless otherwise stated, all matrices and vectors are over GF(2). Matrix multiplication and vector addition are defined as usual, based on "+" and "$\cdot$". 0^k, $[\mathbf{0}]$ and $[\mathbf{1}]$ denote, respectively, the all-zero vector, all-zero matrix and all-one matrix.

Definition 1 A CFSM is called a *linear compacting finite state machine* (L-CFSM) if there exists a $k \times k$ matrix $\mathbf{C}$ such that, for any compactor state s and any test response r, the next state s' of the CFSM is given by $s' = s\mathbf{C} + r$. □

By Definition 1, if the initial state of a L-CFSM is s_0 and a response sequence r_0, r_1, ..., r_{t-1} is applied to it, the resulting state, s_t ($t = 1, 2, \ldots$), can be expressed as follows:

$$s_t = s_0\mathbf{C}^t + \sum_{i=0}^{t-1} r_i\mathbf{C}^i. \tag{1}$$

Every response r_i from the CUT can be considered as the sum of the error-free response, f_i, and an error vector, e_i, i.e., $r_i = f_i + e_i$. For all i, $e_i \in \mathcal{E}$, where $\mathcal{E} = \{\epsilon_0, \epsilon_1, \ldots\}$ denotes the set of all possible error vectors, including 0^k, if the "no-error" vector is also possible, i.e., if the CUT does not produce only faulty outputs. From (1), it follows that

$$s_t = s_0\mathbf{C}^t + \sum_{i=0}^{t-1}(f_i + e_i)\mathbf{C}^i = s_0\mathbf{C}^t + \sum_{i=0}^{t-1} f_i\mathbf{C}^i + \sum_{i=0}^{t-1} e_i\mathbf{C}^i.$$

Notice that $s_0\mathbf{C}^t + \sum_{i=0}^{t-1} f_i\mathbf{C}^i$ corresponds to the L-CFSM state produced by an error-free CUT response sequence. Thus, we have the following.

Proposition 1 *Let e_0, e_1, ..., e_{t-1}, be the error sequence contained in a response sequence of length t. Aliasing error occurs if and only if*

$$\sum_{i=0}^{t-1} e_i\mathbf{C}^i = 0^k \tag{2}$$

and there is an i such that $e_i \neq 0^k$. □

[1] In the rest of the paper, for simplicity, the operator "$\cdot$" will be omitted. Concatenation and power notation will be used instead. Thus, for example, AB will denote $A \cdot B$, and $\mathbf{C}^t$ will denote $\mathbf{C}$ multiplied by itself $t-1$ times.

3.1 Relevant Algebraic Concepts

Our ultimate objective is to find the asymptotic value of the aliasing *probability*. i.e., the probability that (2) is satisfied. First, however, it is useful to discuss only the *possibility* of aliasing, i.e., conditions under which (2) can be satisfied.

If there is no error, then by definition there is no aliasing. Therefore, we assume that $\mathcal{E}$ contains at least one non-zero error vector e. The simplest question that one can ask about the possibility of aliasing is whether eq. (2) can be satisfied by choosing $e_i = 0^k$ or e for each i. In other words, does there exist a non-empty J such that $e\sum_{i\in J}\mathbf{C}^i = 0^k$? This question corresponds to a well-known notion of annihilator from linear algebra.

Definition 2 Given a $k\times k$ matrix $\mathbf{C}$, a polynomial in $\mathbf{C}$, $\alpha(\mathbf{C})$, *annihilates* $e \in \Theta_k - \{0^k\}$ if $e\alpha(\mathbf{C}) = 0^k$. The *annihilator* of $e \in \Theta_k - \{0^k\}$ with respect to $\mathbf{C}$, denoted $\alpha_e(x)$, is the minimum-degree non-zero polynomial such that $\alpha_e(\mathbf{C})$ annihilates e. □

We use annihilator and other concepts and results from linear algebra to solve our problem. Some of them are reviewed next.

Lemma 1 *Given a $k\times k$ matrix $\mathbf{C}$ and a non-zero vector $e \in \Theta_k$, suppose the annihilator of e with respect to $\mathbf{C}$, α_e, has degree m. Then, we have the following:*

(a) *Vectors $e, e\mathbf{C}, \ldots, e\mathbf{C}^{m-1}$ are linearly independent.*

(b) *Any $e\mathbf{C}^i$, where $i \geq 0$, can be expressed as a linear combination of $e, e\mathbf{C}, \ldots, e\mathbf{C}^{m-1}$.*

Proof: (a) Immediately follows from the minimality of the degree of the annihilator.
(b) Since $\alpha_e(\mathbf{C}) = 0$, $e\mathbf{C}^i = e(\mathbf{C}^i \ mod \ \alpha_e(\mathbf{C}))$. The right hand side of this equation is clearly a linear combination of $e, e\mathbf{C}, \ldots, e\mathbf{C}^{m-1}$. □

Definition 3 [2] Given a transition matrix $\mathbf{C}$, the *characteristic polynomial* for $\mathbf{C}$, denoted $\phi(x)$, is given by $|\mathbf{C} - x\mathbf{I}| = 0$, where $\mathbf{I}$ is the identity matrix. The *minimal polynomial* for $\mathbf{C}$, denoted $\mu(x)$, is the polynomial of minimum degree such that $\mu(\mathbf{C}) = [\mathbf{0}]$, where substituting $\mathbf{C}$ for $x^0 = 1$ produces $\mathbf{C}^0$, i.e., the identity matrix $\mathbf{I}$. □

Lemma 2 (a) *$\mu(x)$ divides $\phi(x)$.*

(b) *For all* $e \in \Theta_k - \{0^k\}$, $\alpha_e(x)$ *divides* $\mu(x)$.

Proof: (a) See [2, page 296].

(b) Let

$$\mu(x) = \alpha_e(x)p(x) + q(x), \tag{3}$$

where the degree of $q(x)$ satisfies $deg(q(x)) < deg(\alpha_e(x))$. By substituting $\mathbf{C}$ for x in (3) and multiplying both sides by e, we get

$$e\mu(\mathbf{C}) = e\alpha_e(\mathbf{C})p(\mathbf{C}) + eq(\mathbf{C}).$$

Since $e\mu(\mathbf{C}) = e\alpha_e(\mathbf{C}) = 0^k$ by definition, we have $eq(\mathbf{C}) = 0^k$. From the minimality of the degree of $\alpha_e(x)$, it follows that $q(x) \equiv 0$, i.e., all coefficients of $q(x)$ are 0. □

4 Aliasing in CFSMs

One way of determining the asymptotic value of aliasing probability is applying the theory of ergodic processes [8]. To do so, however, we need to prove some properties of the system we are considering. The most fundamental is the answering of a generalized version of a question posed in section 3.1, i.e.,

Question: For each $v \in \Theta_k$, does there exist an error sequence, $e_0, e_1, \ldots, e_{t-1}$, that satisfies the following equation?

$$\sum_{i=0}^{t-1} e_i \mathbf{C}^i = v \tag{4}$$

□

The following definition will help answer this question.

Definition 4 A $k \times k$ matrix $\mathbf{C}$ has the *singleton generator property* if for all $e(\neq 0^k) \in \Theta_k$ and for all $v \in \Theta_k$ there exists J such that

$$\sum_{i \in J} e\mathbf{C}^i = v.$$

□

Lemma 1(b) implies that if $\mathbf{C}$ has the singleton generator property, then the degree of $\alpha_e(x)$ must be k for all $e \in \Theta_k - \{0^k\}$. Lemma 1(a) then implies that J in Definition 4 can be restricted to $J \subseteq \{0, 1, \ldots, k-1\}$.

4.1 Multiple Error Vectors

Proposition 2 *Suppose* $\mathbf{C}$ *has the singleton generator property and* $\mathcal{E}$ *satisfies* $0^k \in \mathcal{E}$ *and* $|\mathcal{E}| \geq 2$. *Then, for all* $v \in \Theta_k$, *there exists a sequence of error vectors,* $e_0, e_1, \ldots, e_{t-1}$ *such that*

$$\sum_{i=0}^{t-1} e_i \mathbf{C}^i = v.$$

□

In terms of the algebraic concept used in [6], a $k \times k$ transition matrix $\mathbf{C}$ does not have any *invariant subspace* [2, page 302] of dimension d, $0 < d < k$, if and only if it has the singleton generator property. We generalize the above proposition to the case where the condition $0^k \in \mathcal{E}$ is removed. In fact, in the remainder of this paper, we need only assume that $|\mathcal{E}| \geq 2$. Let $\epsilon_0 \in \mathcal{E}$. Rewriting $\sum_{i=0}^{t-1} e_i \mathbf{C}^i$ as

$$\sum_{i=0}^{t-1} e_i \mathbf{C}^i = \sum_{i=0}^{t-1} \epsilon_0 \mathbf{C}^i + \sum_{i=0}^{t-1} (e_i - \epsilon_0) \mathbf{C}^i,$$

we see that eq. (4) can be satisfied if and only if $\sum_{i=0}^{t-1} (e_i - \epsilon_0) \mathbf{C}^i = v'$ can be satisfied for all $v' \in \Theta_k$.

Theorem 1 *Suppose* $\mathbf{C}$ *has the singleton generator property and* $|\mathcal{E}| \geq 2$ *holds. Then, for all* $v \in \Theta_k$, *there exists a sequence of error vectors,* $e_0, e_1, \ldots, e_{t-1}$ *such that*

$$\sum_{i=0}^{t-1} (e_i - \epsilon_0) \mathbf{C}^i = v$$

for any fixed $t \geq k$.

Proof: Let $\epsilon_l \in \mathcal{E}$ be such that $e = \epsilon_l - \epsilon_0 \neq 0^k$. Without loss of generality, we may restrict the error vector sequence such that, for all i, $e_i = \epsilon_0$ or ϵ_l. Then, we have

$$\sum_{i=0}^{t-1} (e_i - \epsilon_0) \mathbf{C}^i = \sum_{i \in J} e \mathbf{C}^i, \tag{5}$$

where $J = \{i \mid e_i \neq \epsilon_0\}$.

Since $\mathbf{C}$ has the singleton generator property, by Proposition 1, any vector $v \in \Theta_k$ can be expressed in the above form, and the remainder of the proof follows from the comments following Definition 4 □

Let the matrix, $\mathbf{C}$, representing a L-CFSM have the singleton generator property. Now, consider the state transition diagram for this L-CFSM, which has 2^k possible states. Out of each state, there are two transitions corresponding to two inputs, 0^k and e. Theorem 1 implies that, in this state transition diagram, there is a path from state 0^k to every other state. Moreover, such a path has length (i.e., the number of edges on it) at most $k-1$.

The following theorem is also proved by Damiani, et al., [6]. A considerably simplified version of their proof will be presented in Section 6. We present here an entirely different proof.

Theorem 2 *Matrix* $\mathbf{C}$ *has the singleton generator property if and only if its characteristic polynomial* $\phi(x)$ *is irreducible.*

Proof:
Only-if: Since $\mathbf{C}$ is a $k \times k$ matrix, the characteristic polynomial of $\mathbf{C}$, $\phi(x)$, has degree k. Assume $\phi(x)$ is reducible, and let $\phi(x) = a(x)b(x)$, where $m = deg(a(x))$ satisfies $1 < m < k$. By the Cayley-Hamilton theorem [2], for all $e \in \Theta_k$, we have

$$e\phi(\mathbf{C}) = ea(\mathbf{C})b(\mathbf{C}) = 0^k.$$

This implies that $a(\mathbf{C})$ annihilates e or $b(\mathbf{C})$ annihilates $ea(\mathbf{C})$. In the former case, by Lemma 1, $\mathbf{C}$ does not have the singleton generator property. In the latter case, note first that $ea(\mathbf{C}) \in \Theta_k$. Again, by Lemma 1, $\mathbf{C}$ does not have the singleton generator property.
If: If $\phi(x)$ is irreducible, then, by Lemma 2(a), we have $deg(\mu(x)) = deg(\phi(x)) = k$. By Lemma 2(b), for all $e \in \Theta_k - \{0^k\}$, $\alpha_e(x)$ must also have degree k. This implies that vectors, e, $e\mathbf{C}$, ..., $e\mathbf{C}^{k-1}$ are linearly independent, and form a basis of Θ_k. It follows that $\mathbf{C}$ has the singleton generator property. □

Probabilistic Implications

A L-CFSM operates deterministically. The fact that the CUT response vectors fed to a L-CFSM have a probability distribution did not play any role in our analysis. We shall now discuss the probabilistic implications of Theorems 1 and 2.

In the context of testing, the input to a L-CSFM at each clock cycle is a vector generated by the CUT. Given a certain distribution of input vectors fed to the CUT, its outputs will have a certain probability distribution, influenced by the faults that may occur in the CUT. Thus, the L-CFSM is driven by probabilistic inputs. Hence, its behavior can be described by a *time-homogeneous Markov process* [8], provided that the inputs at successive clock cycles are statistically independent. The *transition probability matrix*, $\mathbf{P}$, of this Markov process has n rows and n columns, where $n = 2^k$, i.e., the number of states of the L-CFSM. Since the probabilities of all the response vectors occurring in any state must sum to 1, the matrix $\mathbf{P}$ is a *stochastic matrix*. The fact that $\mathbf{P}$ is *doubly stochastic*, i.e., the sum of each column is also 1, follows from the following lemma.

Lemma 3 *Let* $\mathbf{C}$ *be the matrix representing a L-CFSM.* $\mathbf{C}$ *is non-singular (i.e.,* $|\mathbf{C}| \neq 0$*) if and only if, for any state* s *and for any response vector* r*, there exists a unique state* s' *such that* r *causes a transition from* s' *to* s*, i.e.,* $s = s'\mathbf{C} + r$.

Proof: s, r and s' satisfy $s'\mathbf{C} = s - r$. If the components of s' are considered as unknowns, then the above equation is a system of k simultaneous linear equations. If the numbers involved are real, then it is well-known that s' has a unique solution if and only if $\mathbf{C}$ is non-singular [25]. The same proof carries over to the case where the numbers are from $GF(2)$. □

Note that the non-singularity of $\mathbf{C}$ is equivalent to the condition that the characteristic polynomial, $\phi(x)$, have a non-zero constant term. This condition is obviously satisfied if $\phi(x)$ is irreducible.

As before, let us construct the state transition diagram, and label the transition out of each state caused by the response r_j by the probability that r_j is generated by the CUT. Then, Lemma 3 implies that the labels of all incoming arrows to each state sum to 1, i.e., the transition probability matrix $\mathbf{P}$ is doubly stochastic. Therefore, Theorem 2 and Lemma 3, together with Theorem 1, imply the following corollary on *ergodicity* [8].

Corollary 1 *Let* $\mathbf{C}$ *be the matrix representing a L-CFSM. The Markov process represented by the transition probability matrix* $\mathbf{P}$ *is ergodic, if the characteristic polynomial*

of $\mathbf{C}$ *is irreducible and the error vector set* $\mathcal{E}$ *contains at least two vectors that have probabilities different from zero.* □

It is known that, in an ergodic Markov process represented by a doubly stochastic matrix $\mathbf{P}$, the limiting probabilities of all states are equal [8, page 399], which in our case is 2^{-k}. Note that, when there is no error, the L-CFSM ends up in one of its 2^k states, say s. Even if there are errors, the above result implies that the L-CFSM can still end up in s, thus causing aliasing, with probability 2^{-k}. We now are in a position to state the most important result of this paper.

Theorem 3 *Let* $\mathbf{C}$ *be the matrix representing a L-CFSM. If the characteristic polynomial of* $\mathbf{C}$ *is irreducible and the error vector set* $\mathcal{E}$ *contains at least two vectors that have probabilities different from zero, then the probability of aliasing converges to* 2^{-k}. □

4.2 Single Error Vector

As we saw in the previous subsection, if at least two error vectors have probability different from zero, then L-CFSMs with irreducible characteristic polynomials have more desirable aliasing property than those characterized by reducible polynomials. Thus, our analysis of single error case will be confined to L-CFSMs with irreducible characteristic polynomials.

It is known (and follows from Lemma 3) that the states of a L-CFSM, represented by non-singular matrix C, form cycles [1]. More precisely, for any state, the previous and the next state are uniquely defined, when a constant input vector is applied to the L-CFSM inputs. Subsequently, the state cycles formed under constant input vector $r = 0^k$ will be referred to as the *primary state cycles.* Naturally, if state s belongs to a primary state cycle of length m, then $s\mathbf{C}^m = s$.

Theorem 4 *Suppose a L-CFSM is described by a* $k \times k$ *matrix* $\mathbf{C}$ *whose characteristic polynomial is irreducible. If a single error vector,* e*, is applied to the L-CFSM inputs at every clock cycle, then aliasing occurs at time* t *if and only if* t *is a multiple of the length of the primary state cycle containing* e.

Proof: In the single error case, by Proposition 1, aliasing occurs if and only if $\sum_{i=0}^{t-1} e\mathbf{C}^i = 0^k$. It is easy to see that

$$(\sum_{i=0}^{t-1} \mathbf{C}^i)(\mathbf{C}+\mathbf{I}) = \mathbf{C}^t + \mathbf{I}.$$

Multiplying the above equation by e from the left, we obtain

$$(\sum_{i=0}^{t-1} e\mathbf{C}^i)(\mathbf{C}+\mathbf{I}) = e\mathbf{C}^t + e. \tag{6}$$

Only if: It follows from Eq. (6) that, if $\sum_{i=0}^{t-1} e\mathbf{C}^i = 0^k$ then $e\mathbf{C}^t = e$, which implies that the L-CFSM returns to state e after t transitions.

If: It follows from Eq. (6) that if $e\mathbf{C}^t = e$, then either (i) $\sum_{i=0}^{t-1} e\mathbf{C}^i = 0^k$, or (ii) $e' \neq 0^k$ and $e'\mathbf{C} = e'$, where $e' = \sum_{i=0}^{t-1} e\mathbf{C}^i$. In case (i), clearly, aliasing occurs at time t.

In case (ii), we need to deal with the two subcases, $k = 1$ and $k > 1$. If $k = 1$, then the only nontrivial case is where $\mathbf{C} = [\mathbf{1}]$, and $e'\mathbf{C} = e'$ holds for both $e' = 0$ and $e' = 1$. This means that aliasing occurs at any time.

If $k > 1$, then by Lemma 2, the annihilator for e', $\alpha_{e'}(x)$, must divide the characteristic polynomial of $\mathbf{C}$, $\phi(x)$. Since $\phi(x)$ is irreducible, $deg(\alpha_{e'}(x)) = k$, which implies that $e'(\mathbf{C}+\mathbf{I}) = 0$ cannot happen.

□

Theorem 4 says that, in the case of irreducible polynomials, one can determine the times when aliasing is possible by analyzing the structure of the primary state cycles. This analysis may be simplified by using the following lemma.

Lemma 4 [1, page 70] Let σ be any primary state cycle. If the characteristic polynomial of the L-CFSM is irreducible of degree k, then the length of σ is a factor of $2^k - 1$.

Some C-LFSMs are characterized by *primitive polynomials* which constitute a subset of irreducible polynomials. Such L-CFSMs are known to have exactly two primary cycles; one of length 1, consisting only of the zero state, and the other containing all the the non-zero states. Thus, if the characteristic polynomial is primitive, for any single error distribution, aliasing can only occur exactly at times that are multiples of $2^k - 1$. Such test running time should be avoided to minimize aliasing.

5 Discussion

Since a *linear feedback shift register* (LFSR) [21]. is popular as a test compactor as well as for other purposes, here, we shall interpret Theorem 2 in terms of LFSRs.

Let **D** be a matrix which has zero elements as shown below.

$$\mathbf{D} = \begin{pmatrix} 0 & 1 & \cdot & \cdot & 0 & 0 \\ 0 & 0 & \cdot & \cdot & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & 0 & 1 \\ d_0 & d_1 & \cdot & \cdot & d_{k-2} & d_{k-1} \end{pmatrix} \tag{7}$$

We first consider the special case where the given L-CFSM is a LFSR, namely, its transition matrix **C** has the same form as **D**. Then, it is easy to see that **C** has the following characteristic polynomial.

$$\phi(x) = d_0 + d_1 x + \ldots + d_{k-2} x^{k-2} + d_{k-1} x^{k-1} + x^k.$$

$\phi(x)$ is called the *generator polynomial* of the LFSR. As is well-known [21], for any state $e = (e_0, e_1, \ldots, e_{k-1}) \in \Theta^k$, e and $e\mathbf{C}$ of the LFSM can be represented by $e(x)$ and $xe(x)$ *mod* $\phi(x)$, respectively, where

$$e(x) = e_0 + e_1 x + \ldots + e_{k-1} x^{k-1}.$$

Therefore, the singleton generator property of **C** is equivalent to the linear independence (*mod* $\phi(x)$) of k polynomials

$$e(x), xe(x), \ldots, x^{k-1}e(x),$$

for all $e(x)$ with $deg(e(x)) \leq k-1$.

Assume that these k polynomials are linearly *dependent*. Then there is a non-zero polynomial $a(x)$ with $deg(a(x)) \leq k-1$ such that $a(x)e(x) = 0$ *mod* $\phi(x)$, which implies that $a(x)e(x)$ divides $\phi(x)$. This is *not* possible for all $e(x)$ with $deg(e(x)) \leq k-1$, if and only if $\phi(x)$ is irreducible, since $deg(\phi(x)) = k$ and both $e(x)$ and $a(x)$ have degree less than k. It follows that **C** has the singleton generator property if and only if $\phi(x)$ is irreducible.

We now consider the general case where the transition matrix $\mathbf{C}$ of the given L-CFSM is not necessarily of the form (7). It turns out that if the characteristic polynomial of $\mathbf{C}$ is irreducible, then the behavior of the L-CFSM is "mimicked" by a LFSR, so that it still is the case that $\mathbf{C}$ has the singleton generator property if and only if $\phi(x)$ is irreducible. The following lemma provides the crucial property of transition matrices with irreducible characteristic polynomials.

Lemma 5 [17] *If the characteristic polynomial, $\phi(x)$, of $\mathbf{C}$ is irreducible, then there exists a $k \times k$ non-singular matrix $\mathbf{T}$ such that $\mathbf{D} = \mathbf{T}^{-1}\mathbf{C}\mathbf{T}$ (i.e., $\mathbf{D}$ and $\mathbf{C}$ are similar), where $\mathbf{D}$ is the matrix given in (7).*

□

As observed by Damiani, et al. [6], since $\mathbf{T}$ is an *automorphism* from Θ_k to itself, $\mathbf{C}$ has the singleton generator property if and only if $\mathbf{D}$ does likewise. Since we have already shown above that $\mathbf{D}$ has the singleton generator property, it follows that $\mathbf{C}$ also has the singleton generator property.

In proving their restricted version of Theorem 3, Daehn, et al. [4], make use of earlier results presented for a single-input signature register. Then, using D-transforms, a correspondence between single-input and multiple-input signature registers is established. Such correspondence provides a basis for a property concerning the ergodicity of the Markov process that describes the behavior of multiple-input signature registers when more then two error vectors appear at the outputs of the CUT.

6 Concluding Remarks

We have shown that if the characteristic polynomial of a linear compacting finite state machine is irreducible, then the aliasing probability tends asymptotically to 2^{-k}, where k is the number of binary memory elements of the L-CFSM, provided that at least two error vectors occur with non-zero probabilities. Our result is a generalization of results presented in [4] and [6] in that it is valid without the assumption that the "no-error" pattern has a non-zero probability. We have also determined what test length should be avoided to minimize aliasing by faults that produce exactly one error vector.

As discussed in section 2, we believe that, from a practical point of view, the results presented in [4, 6] and discussed in these notes provide the most fundamental information on aliasing probability with L-CFSM derived so far.

References

[1] P. H. Bardell, W. H. McAnney, and J. Savir, *Built-In Test for VLSI: Pseudorandom Techniques,* New York: John Wiley & Sons, Inc., 1987.

[2] G. Birkhoff and S. MacLane, *A Survey of Modern Algebra,* 3d ed., New York: Macmillan, 1965.

[3] W. C. Carter, "The Ubiquitous Parity Bit," *Proc. FTCS-12,* June 1982, pp. 289-296.

[4] W. Daehn, T. W. Williams and K. D. Wagner, "Aliasing Errors in Linear Automata Used as Multiple-Input Signature Analyzers," *IBM Journal of Research and Development,* Vol. 34, No. 2/3, Mar./May 1990, pp. 363-380.

[5] M. Damiani, P. Olivo, M. Favalli, S. Ercolani, and B. Riccó, "Aliasing in Signature Analysis Testing with Multiple-Input Shift Registers," *Proc. European Test Conf.,* Apr. 1989, pp. 346-353.

[6] M. Damiani, P. Olivo, and B. Riccó, "Analysis and Design of Linear Finite State Machines for Signature Analysis Testing," *IEEE Trans. Comput.,* to appear.

[7] R. David, "Comments on 'Signature Analysis for Multiple Output Circuits," *IEEE Trans. Comput.,* Vol. 39, No. 2, Feb. 1990, pp. 287-288.

[8] W. Feller, *An Introduction to Probability Theory and Its Applications,* Vol. 1, New York: John Wiley and Sons, Inc., 1950.

[9] R. A. Frohwerk, "Signature Analysis: A New Digital Field Service Method," *Hewlett-Packard Journal,* May 1977, pp. 2-8.

[10] H. Fujiwara, *Logic Testing and Design for Testability,* Boston, MA: MIT Press, 1985.

[11] S. Z. Hassan, D. J. Lu, and E.J. McCluskey, "Parallel Signature Analyzers – Detection Capability and Extensions," *26th IEEE Computer Society Int. Conf, COMPCON Spring 83,* Feb.-Mar. 1983, pp. 440-445.

[12] J. P. Hayes, "Check Sum Test Methods," *Proc. FTCS-6,* June 1976, pp. 114-119.

[13] A. Hlawiczka, "Hybrid Design of Parallel Signature Analyzers," *Proc. European Test Conf.,* Apr. 1989, pp. 354-360.

[14] P. D. Hortensius, R. D. McLeod, W. Pries, D. M. Miller, and H. C. Card, "Cellular Automata-Based Pseudorandom Number Generators for Built-In Self-Test," *IEEE Trans. CAD,* Vol. 8, No. 8, Aug. 1989, pp. 842-859.

[15] K. Iwasaki and F. Arakawa, "An Analysis of the Aliasing Probability of Multiple-Input Signature Registers in the Case of a 2^m-ary Symmetric Channel," *IEEE Trans. CAD,* Vol. 9, No. 4, Apr. 1990, pp. 427-438.

[16] E. J. McCluskey, *Logic Design Principles with Emphasis on Testable Semicustom Circuits,* Englewood Cliffs, NJ: Prentice-Hall, 1986.

[17] C.C. McDuffee, *Vectors and Matrices,* Ithaca, N.Y.: Math. Assoc. of America, 1961.

[18] D. M. Miller and S. Zhang, "Aliasing in Multiple-Input Data Compactors," *Proc. Canadian Conf. on Electrical and Computer Eng.,* Sept. 1989, pp. 347-351.

[19] J. C. Muzio, F. Ruskey, R. C. Aitken, and M. Serra, "Aliasing Probabilities for Some Data Compression Techniques," *Developments in IC Testing,* D. M. Miller, ed., London: Academic Press, 1987.

[20] K. P. Parker, "Compact Testing: Testing with Compressed Data," *Proc. FTCS-6,* June 1976, pp. 93-98.

[21] W. W. Peterson and E. J. Welson, *Error-Correcting Codes,* Cambridge MA: MIT Press, 1972.

[22] D. K. Pradhan, S. K. Gupta, and M. G. Karpovsky, "Aliasing Probability for Multiple Input Signature Analyzer," *IEEE Trans. Comput.,* Vol. 39, No. 4, Apr. 1990, pp. 586-592.

[23] J. P. Robinson and N. R. Saxena, "Simultaneous Signature and Syndrome Compression," *IEEE Trans. CAD,* Vol. 7, No. 5, May 1988. (pp.??)

[24] T. Sridhar, D. S. Ho, T. J. Powell, and S. M. Thatte, "Analysis and Simulation of Parallel Signature Analyzers," *Int. Test Conf.,* Philadelphia, Nov. 1982, pp. 656-661.

[25] G. Strang, *Linear Algebra and Its Applications, 3rd ed.,* Sandiego: Harcourt Brace Jovanovich, 1988.

[26] L. T. Wang and E. J. McCluskey, "Hybrid Designs Generating Maximum-Length Sequences," *IEEE Trans. CAD,* Vol. 7, No. 1, Jan. 1988, pp. 91-99.

[27] T. W. Williams and W. Daehn, "Aliasing Probability for Multiple Input Signature Analyzers with Dependent Inputs," *Proc. CompEuro 89,* Hamburg, May 1989, pp. 5-120–5-127.

[28] T. W. Williams and W. Daehn, "Aliasing Errors in Multiple Input Signature Analysis Registers," *Proc. European Test Conf.,* Apr. 1989, pp. 338-345.

[29] T. W. Williams, W. Daehn, M. Gruetzner, and C. W. Starke, "Comparison of Aliasing Errors for Primitive and Non-Primitive Polynomials," *Proc. ITC,* Sept. 1986, pp. 282-288.

[30] Y. Zorian and V. K. Agarwal, "A General Scheme to Optimize Error Masking in Built-In Self-Testing," *Proc. FTCS-16,* July 1986, pp. 410-415.

[31] Proposed IEEE P1149.1 Standard Test Access Port and Boundary-Scan Architecture, Draft D3, Jan. 18, 1989.

[32] "The Challenges of Self-Test," *IEEE Design & Test Mag.*, Feb. 1990, pp. 46-56.

Centre for Systems Science

• Simon Fraser University established the **Centre for Systems Science** as a provincial centre for advanced study. The objective of CSS is twofold: coordinate and combine advanced systems research at SFU, and encourage application of research results within industry in order to further the technological development of British Columbia.

•CSS has assembled three research groups to streamline its efforts. The orientation of these groups is as follows: intelligent systems, microelectronics, and computer and communications systems. Because of shared research interests, this latter group merges with LCCR (**Laboratory for Computer and Communications Research**) for the publication of technical reports.

• CSS's three groups involve over 80 skilled faculty researchers principally from SFU's Schools of Engineering Science and Computing Science, but also draw substantially on Mathematics, Physics, Geography, Philosophy, Linguistics, Psychology, Communication, and Kinesiology.